COVID-19: UN DESAFÍO PARA LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

COVID-19: A CHALLENGE FOR THE PERSONAL DATA PROTECTION

Actualidad Jurídica Iberoamericana Nº 12 bis, mayo 2020, ISSN: 2386-4567, pp. 860-867

Alfonso
ORTEGA
GIMÉNEZ

ARTÍCULO RECIBIDO: 9 de mayo de 2020
ARTÍCULO APROBADO: 10 de mayo de 2020

RESUMEN: El COVID-19 está permitiendo la adopción de todo tipo de medidas excepcionales que no serían justificadas en una situación de estado normal, siempre que se mantenga un correcto equilibrio entre la prevención de contagios y la recogida, tratamiento y cesión de datos de carácter personal que puedan promover la identificación de personas concretas. La protección de datos de carácter personal ni es ni puede ni debe ser un obstáculo para la más efectiva de las luchas contra el Coronavirus, sino que, en este escenario, las medidas que se adopten en materia de protección de datos de carácter personal deben adoptarse desde la «normalidad jurídica».

PALABRAS CLAVE: COVID-19; protección de datos personales; RGPD; datos relativos a la salud.

ABSTRACT: *COVID-19 is allowing the adoption of all kinds of exceptional measures that would not be justified in a normal state situation, provided that a correct balance is maintained between the prevention of infections and the collection, treatment and transfer of personal data that can promote the identification of specific people. Personal data protection is not, can´t and shouldn´t be an obstacle to the most effective fight against the Coronavirus, but, in this scenario, the measures adopted in the field of protection of personal data must be adopted from "legal normality".*

KEY WORDS: *COVID-19; personal data protection; GDPR; health data.*

1. A medida que el brote de Coronavirus (COVID-19) continúa propagándose, las empresas están implementando un número creciente de medidas para prevenir que la pandemia se propague. Estas medidas a veces requieren que se recopile, analice y comparta información sobre individuos, para cumplir con las normas de Salud y Seguridad, pero plantea un desafío para la Protección de datos de carácter personal: ¿Qué tipos de datos personales se pueden recopilar y cómo? ¿Pueden ser compartidos con empresas del grupo y con entidades externas al grupo como proveedores de servicios y autoridades? ¿La empresa puede obligar al trabajador a decir si tiene Coronavirus? ¿La empresa puede obligar al trabajador a acudir al servicio de prevención o al médico? ¿La empresa puede revelar la identidad del trabajador infectado, si la conoce? ¿Qué se nos puede exigir a todos, trabajadores y empleadores? Estas preguntas surgen en la relación empleador-empleado, pero también surgen cuando se trata con otras partes interesadas que están en contacto con el lugar de trabajo: clientes, proveedores, colaboradores, etc.

2. El COVID-19 ha desatado una serie de medidas excepcionales que ayuden a los distintos países afectados a controlar y tratar de minimizar la propagación del virus a niveles incontrolables. Entre dichas medidas excepcionales nos encontramos, en su extremo más radical, las medidas de control masivo de la ciudadanía que China lleva aplicando durante un tiempo y que han ayudado, gracias al Big Data y a la inteligencia artificial, a restringir los movimientos de sus ciudadanos y contener la propagación del virus. Las medidas de China serían impensables e irrealizables en el resto del mundo, la propagación mundial del Coronavirus ha puesto en marcha protocolos de contención y control en la mayoría de países, con mejor o peor acierto desde el punto de vista de la Protección de Datos de Carácter Personal de los afectados.

3. Sin duda, este tipo de medidas excepcionales no serían toleradas en una situación de estado normal, pero en casos de potenciales pandemias sí podrían estar justificadas siempre que se mantenga un correcto equilibrio entre la prevención de contagios y la recogida, tratamiento y cesión de datos de carácter personal que puedan promover la identificación de personas concretas.

• Alfonso Ortega Giménez
Profesor Contratado Doctor de Derecho internacional privado de la Universidad Miguel Hernández de Elche (acreditado a Profesor Titular de Universidad). Correo electrónico: alfonso.ortega@umh.es

En España, durante la primera semana del pasado mes de marzo ya tuvimos un primer «desequilibrio» en este sentido, y es que Fernando Simón -Director del Centro de Alertas y Emergencias Sanitarias del Ministerio de Sanidad- señaló a una Iglesia Evangélica de Torrejón de Ardoz (Madrid) como posible núcleo de infección ya que dijo que «se habían identificado varios casos» y añadió que «se estaba investigando la posible relación con otras personas que pertenecen a otros grupos religiosos equivalentes».

Si bien son 19 las iglesias evangélicas en Torrejón, y esto no permite identificar de manera inequívoca a personas concretas, la Federación de Entidades Religiosas Evangélicas de España ha expresado su malestar porque indican que «se han sentido señalados y se ha estigmatizado a una comunidad religiosa».

Además, muchas empresas de zonas de riesgo (Madrid, País Vasco o Comunidad Valenciana) comenzaron a tomar por su cuenta medidas de prevención en los controles de acceso a sus empleados, con preguntas como si han viajado recientemente, si tienen tos o dolor de cabeza, etc. En función a las respuestas, las mismas personas responsables del control de acceso, son quienes están decidiendo en algunos casos si el trabajador, cliente, proveedor, etc. podía entrar o no a sus instalaciones.

4. En el Reglamento General de Protección de Datos de la Unión Europea (RGPD), su artículo 9.1 establece, como base, la prohibición del tratamiento de datos sensibles, entre los que se encuentran los datos relativos a la salud. Posteriormente se aclaran algunas excepciones a dicha prohibición, en su artículo 9.2, donde cabe mencionar las siguientes: « […] c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3; i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados

niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional[…]».

Además, el propio RGPD aclara en el punto 9.3 que «dicho tratamiento debe ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión […]». Este aspecto se ha de complementar con lo que refleja el artículo 33.2.h de la Ley 33/2011 General de Salud Pública, que indica: «La autoridad sanitaria, de forma coordinada con la autoridad laboral, llevará a cabo las siguientes actuaciones además de las ya establecidas normativamente: […] h) Establecer mecanismos de coordinación en caso de pandemias u otras crisis sanitarias, en especial para el desarrollo de acciones preventivas y de vacunación».

Así las cosas, corresponde únicamente a la autoridad sanitaria determinar qué medidas se aplicarán en el ámbito laboral, y siempre por parte de un profesional sujeto a la obligación del secreto profesional. Si dicha autoridad indicara a una empresa en este escenario excepcional que nos encontramos, que recabe este tipo de datos de sus trabajadores o de las visitas que pudiera recibir, sí podríamos llegar a hablar de un tratamiento legítimo, lícito y justificable, aunque habría que revisar el escenario concreto y qué medidas ha tomado esa empresa para hacer un tratamiento conforme al reglamento.

El hecho de que el personal de la empresa recabe o trate datos relativos a la salud bajo las indicaciones de cualquier mando de la empresa supone una violación del artículo 9.1 del RGPD y vulneración del principio de proporcionalidad, que además podría dar lugar a filtraciones y/o brechas de seguridad graves debido a la falta de responsabilidad corporativa, al ser un caso de tratamiento de datos de riesgo sin las medidas de seguridad oportunas, ni la formación ni preparación correspondiente para el personal que la realiza.

Lo que sí pueden hacer las empresas por su cuenta, en caso de que los mandos decidan aplicar algún tipo de medida, es implementar protocolos de actuación preventiva donde no se recaben este tipo de datos, como, por ejemplo, evitar la asistencia al trabajo en caso de tener determinados síntomas, lavarse las manos habitualmente y evitar el contacto personal, o aplicar el teletrabajo a todo el porcentaje posible de la plantilla si eso no merma el normal desempeño de sus funciones.

5. La Agencia Española de Protección de Datos (AEPD) ha publicado un informe en el que analiza el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19. El RGPD contiene las reglas necesarias para permitir legítimamente tratamientos de datos personales en situaciones en las que existe una emergencia sanitaria de alcance general. En consecuencia, según se recoge en el informe, la protección de datos de carácter personal no debería utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la pandemia.

El informe recoge que el RGPD reconoce explícitamente en su Considerando 46 como base jurídica para el tratamiento lícito de datos personales en casos excepcionales, como el control de epidemias y su propagación, la misión realizada en interés público (art. 6.1.e) o los intereses vitales del interesado u otras personas físicas (art. 6.1.d), sin perjuicio de que puedan existir otras bases como, por ejemplo, el cumplimiento de una obligación legal (para el empleador en la prevención de riesgos laborales de su personal). Estas bases jurídicas permiten el tratamiento de datos sin consentimiento de los afectados.

Los datos de salud están catalogados en el RGPD como categorías especiales de datos, prohibiéndose su tratamiento salvo que pueda ampararse en alguna de las excepciones recogidas en la normativa. El informe precisa las excepciones recogidas en el art. 9.2. RGPD:

- El cumplimiento de obligaciones en el ámbito del Derecho laboral y de la seguridad y protección social (art. 9.2.b). El informe recuerda la obligación de empleadores y de su personal en materia de prevención de riesgos laborales, y que corresponde a cada trabajador velar por su propia seguridad y salud en el trabajo y por la de aquellas personas a las que pueda afectar su actividad profesional a causa de sus actos y omisiones en el trabajo. Ello supone que el personal deberá informar a su empleador en caso de sospecha de contacto con el virus, a fin de salvaguardar, además de su propia salud, la de los demás trabajadores del centro de trabajo para que se puedan adoptar las medidas oportunas.

- El interés público en el ámbito de la salud pública (art. 9.2.i), que en este caso se configura como interés público esencial (art. 9.2.g).

- Cuando sea necesario para la realización de un diagnóstico médico (art. 9.2.h).

- Cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otras personas, cuando el interesado no esté capacitado para prestar su consentimiento. (art. 9.2.c).

Por otro lado, el informe hace referencia a la Ley Orgánica 3/1986 de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo) o la Ley 33/2011 General de Salud Pública. La primera de dichas normas señala que "con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible".

En materia de riesgo de transmisión de enfermedades, epidemia, crisis sanitarias, etc., la normativa aplicable ha otorgado a las autoridades sanitarias de las distintas AAPP las competencias para adoptar las medidas necesarias previstas por la ley cuando así lo exijan razones sanitarias de urgencia o necesidad. Desde un punto de vista de tratamiento de datos personales, la protección de los intereses vitales de las personas físicas corresponde en el ámbito de la salud a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las medidas necesarias para salvaguardar a las personas en situaciones de emergencia sanitaria.

Así, serán las autoridades sanitarias de las distintas Administraciones Públicas quienes deberán adoptar las decisiones necesarias, y los distintos responsables de los tratamientos de datos personales deberán seguir dichas instrucciones, incluso cuando ello suponga un tratamiento de datos personales de salud.

Del mismo modo, y en aplicación de lo establecido en la normativa de trabajo y de prevención de riesgos laborales, los empleadores podrán tratar, de acuerdo con dicha normativa y con las garantías que dichas normas establecen, los datos necesarios para garantizar la salud de todo su personal, y evitar contagios en el seno de la empresa y/o centros de trabajo.

Por último, el informe destaca que los tratamientos de datos personales, aún en estas situaciones de emergencia sanitaria, deben seguir siendo tratados de conformidad con la normativa de protección de datos personales (= RGPD y Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)), ya que estas normas han previsto esta eventualidad, por lo que le son de aplicación sus principios, y entre ellos el de tratar los datos personales con licitud, lealtad y transparencia, limitación de la finalidad (en este caso, salvaguardar los intereses de las personas ante esta situación de pandemia), principio de exactitud, y el principio de minimización de datos. Sobre esto último, se hace una referencia expresa a que los datos tratados habrán de ser exclusivamente los limitados a los necesarios para la finalidad pretendida, sin que

se pueda extender dicho tratamiento a otros datos personales no estrictamente necesarios para dicha finalidad.

6. Así las cosas, opino que, en estos momentos, no podamos pensar que el derecho fundamental a la protección de datos de carácter personal esté vaciándose de contenido, ya que, como se ha señalado, tanto el RGPD como la Ley Orgánica de Protección de Datos (LOPDGDD) permiten el tratamiento de datos, incluidos datos relativos a la salud, sin el consentimiento de los afectados cuando sea necesario para atajar el COVID-19. Es más, la protección de datos de carácter personal ni es ni puede ni debe ser un obstáculo para la más efectiva de las luchas contra el Coronavirus, sino que, en este escenario, las medidas que se adopten en materia de protección de datos de carácter personal deben adoptarse desde la «normalidad jurídica», respetando, en todo caso, los principios que enumera el artículo 5 del RGPD (= licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; seguridad en términos de integridad y confidencialidad de los datos y responsabilidad proactiva). Tales medidas han de ser temporales, para finalidades determinadas, que impliquen el acceso limitado a los datos que sean imprescindibles. Y todo ello bajo la atenta supervisión de las autoridades de protección de datos; (en nuestro caso, de la AEPD) cuyas competencias en este ámbito, por lo demás, en ningún caso pueden ser sustraídas ni ejercidas por las autoridades competentes delegadas, pues la existencia misma de una autoridad de control independiente forma asimismo parte del contenido esencial del derecho a la protección de datos, tal como se desprende del artículo 8.3 de la Carta de los Derechos Fundamentales de la Unión Europea.

En definitiva, el desafío del COVID-19 para la protección de datos de carácter personal es simple: debemos estar ante lo que no es más que la «aplicación normal» del marco jurídico que regula el derecho fundamental a la protección de datos de carácter personal.